UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,083	03/31/2004	David Y. Jao	MS1-1956US	9450

22801 7590 03/17/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,083	JAO ET AL.	
	Examiner	Art Unit	
	Martin Jeriko P. San Juan	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/31/2004, 11/12/2004, 1/03/2005, 1/05/2005, 12/28/2005-1, 12/28/2005-2*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Non-Provisional Application filed on March 31, 2004.

This application claims priority from Provisional Application 60/517142 filed on November 3, 2003.

Claims 1-39 are currently pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 28-39 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims fail to place the invention squarely within one statutory class of invention. At Par 0115 and Par 0117 of the instant specification, applicant has provided evidence that applicant intends the "medium" to include signals. As such, the claim is drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim(s) is/are not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or

manufacture. Energy is not a combination of substances and therefore not a composition of matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 2, 4, 8, 10, 13, 14, 16, 20, 23-25, 28, 29, 31, 36, and 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Futa et al. [US 2003/0081771 A1], hereinafter Futa.

Regarding claim 1, Futa teaches a method comprising: generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve [US 2003/0081771 A1, Pg 8, Par 0154]; publishing a public key corresponding to the isogeny [US 2003/0081771 A1, Pg 1, Par 0015] [US 2003/0081771 A1, Pg 3, Par 055] [US 2003/0081771 A1, Pg 3, Par 0063]; encrypting a message using a encryption key corresponding to the isogeny [US 2003/0081771 A1, Pg 11, Par 0206]; and decrypting

the encrypted message using a decryption key corresponding to the isogeny [US 2003/0081771 A1, Pg 11, Par 0206].

Regarding claim 2, Futa teaches a method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key [US 2003/0081771 A1, Pg 1, Par 0016], the private key being a dual isogeny of the isogeny [US 2003/0081771 A1, Pg 8, Par 0154].

Regarding claim 4, Futa teaches a method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves [US 2003/0081771 A1, Pg 10, Par 0197].

Regarding claim 8, Futa teaches a method as recited by claim 1, wherein the method signs the message [US 2003/0081771 A1, Pg 11, Par 0206].

Regarding claim 10, Futa teaches a method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves [US 2003/0081771 A1, Par 0154].

Regarding claim 13, Futa teaches a method comprising: publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve [US 2003/0081771 A1, Pg 8, Par 0154] [US 2003/0081771 A1,

Pg 1, Par 0015] [US 2003/0081771 A1, Pg 3, Par 0055] [US 2003/0081771 A1, Pg 3, Par 0063]; and decrypting an encrypted message using a decryption key corresponding to the isogeny [US 2003/0081771 A1, Pg 11, Par 0206].

Claim 23 is rejected because it is similar subject matter as claim 1.

Claims 14, 24, and 29 are rejected because it is similar subject matter as claim 2.

Claims 16, 25, and 31 are rejected because it is similar subject matter as claim 4.

Claims 20, and 38 are rejected because it is similar subject matter as claim 8.

Claims 28, and 36 are rejected because it is similar subject matter as claims 13, and 10 respectively.

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 1-5, 7-17, 19-26, 28-32, and 34-39 are rejected under 35 U.S.C. 102(a) as being anticipated by Anonymous [NPL, Anonymous, November 2003].

Regarding claim 1, Anonymous teaches a method comprising: generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; publishing a public key corresponding to the isogeny; encrypting a message using a encryption key corresponding to the isogeny; and decrypting the encrypted message

using a decryption key corresponding to the isogeny. [Anonymous, November 2003, Pg 1-3]

Regarding claim 2, Anonymous teaches a method as recited by claim 1, wherein at least one of the encryption key or the decryption key is a private key, the private key being a dual isogeny of the isogeny. [Anonymous, November 2003, Pg 1-3]

Regarding claim 3, Anonymous teaches a method as recited by claim 1, wherein the isogeny is generated using a technique selected from a group comprising modular generation, complex multiplication generation, linearly independent generation, and combinations thereof. [Anonymous, November 2003, Pg 5-8]

Regarding claim 4, Anonymous teaches a method as recited by claim 1, wherein the generating maps a plurality of points from a first elliptic curve onto a plurality of elliptic curves. [Anonymous, November 2003, Pg 1-3]

Regarding claim 5, Anonymous teaches a method as recited by claim 1, wherein the decrypting is performed by bilinear pairing. [Anonymous, November 2003, Pg 4]

Regarding claim 7, Anonymous teaches a method as recited by claim 1, wherein the method is applied using Albelian varieties. [Anonymous, November 2003, Pg 1-3 --

Examiner notes that Albelian varieties are inherent in generating isogenous elliptic curves as taught by Anonymous.]

Regarding claim 8, Anonymous teaches a method as recited by claim 1, wherein the method signs the message. [Anonymous, November 2003, Pg 10]

Regarding claim 9, Anonymous teaches a method as recited by claim 1, wherein the method provides identity based encryption. [Anonymous, November 2003, Pg 11].

Regarding claim 10, Anonymous teaches a method as recited by claim 1, further comprising composing a plurality of modular isogenies to provide the isogeny without revealing any intermediate curves. [Anonymous, November 2003, Pg 7]

Regarding claim 11, Anonymous teaches a method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny. [Anonymous, November 2003, Pg 11]

Regarding claim 12, Anonymous teaches a method as recited by claim 1, further comprising using a trace map to shorten points on an Albelian variety. [Anonymous, November 2003, Pg 11 --Examiner notes that an Albelian variety is inherent in generating isogenous elliptic curves as taught by Anonymous.]

Regarding claim 13, Anonymous teaches a method comprising: publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve; and decrypting an encrypted message using a decryption key corresponding to the isogeny. [Anonymous, November 2003, Pg 1-3]

Claim 23 is rejected because it is similar subject matter as claim 1.

Claims 14, 24, and 29 are rejected because it is similar subject matter as claim 2.

Claims 15, and 30 are rejected because it is similar subject matter as claim 3.

Claims 16, 25, and 31 are rejected because it is similar subject matter as claim 4.

Claims 17, 26, and 32 are rejected because it is similar subject matter as claim 5.

Claims 19, and 34 are rejected because it is similar subject matter as claim 7.

Claims 20, and 38 are rejected because it is similar subject matter as claim 8.

Claims 21, and 39 are rejected because it is similar subject matter as claim 9.

Claims 22, and 35 are rejected because it is similar subject matter as claim 11.

Claim 37 is rejected because it is similar subject matter as claim 12.

Claims 28, and 36 are rejected because it is similar subject matter as claims 13, and 10 respectively.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 3, 7, 15, 19, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, and further in view of Katsura [NPL, Katsura 1975].

Regarding claim 3, Futa teaches a method as recited by claim 1, wherein the isogeny is generated using a technique selected from a group comprising modular generation [US 2003/008177 A1, Pg 8, Par 0154]. Futa does not explicitly teach techniques using complex multiplication generation, linearly independent generation, and combinations thereof.

Katsura teaches generating isogenies using complex multiplication [Katsura 1975, Pg 224], linearly independent generation [Katsura 1975, Pg 226], and combinations thereof [Katsura 1975, Pg 224-228].

It would have been obvious to one of ordinary skilled in the art at the time of invention to combine the different techniques of generating isogenous curves as taught by Katsura. The suggestion/motivation for combining would have been to have various techniques for generating isogenous curves. Katsura is an analogous art because it is in the same field of generating isogenous curves.

Regarding claim 7, Futa and Katsura teaches a method as recited by claim 1, wherein the method is applied using Abelian varieties [Katsura 1975, Pg 224 --Examiner notes that an Abelian variety becomes an inherent property when performing the above techniques of generating isogenies.].

Claims 15, and 30 are rejected because it is similar subject matter as claim 3.
Claims 19, and 34 are rejected because it is similar subject matter as claim 7.

2. Claims 5, 9, 11, 17, 21, 22, 26, 35, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, and further in view of Boneh et al. [US 7113594 B2], hereinafter Boneh.

Regarding claim 5, Futa teaches a method as recited by claim 1.
Futa does not teach wherein the decrypting is performed by bilinear pairing.

Boneh teaches a method for identity based encryption wherein the decrypting is performed by bilinear pairing [US 7113594 B2, Col 3, Ln 4-12].

It would have been obvious to combine identity based encryption into the encryption method of Futa utilizing an elliptic curve generating device. The suggestion/motivation is to have the flexibility of being able to send an encrypted message to a recipient whose public key has not yet been generated and published [US 7113594 B2, Col 1, Ln

51-57]. Boneh is an analogous art because it is in the field of encryption whose method can be derived from an elliptic curve when using Weil or Tate pairing.

Regarding claim 9, Futa and Boneh teaches a method as recited by claim 1, wherein the method provides identity based encryption [US 7113594 B2, Col 10, Ln 23].

Regarding claim 11, Futa and Boneh teach a method as recited by claim 1, further comprising using a trace map down to a base field to shorten points on an elliptic curve mapped by the isogeny [US 7113594 B2, Col 22, Ln 27-49].

Claims 17, 26, and 32 are rejected because it is similar subject matter as claim 5.
Claims 21, and 39 are rejected because it is similar subject matter as claim 9.
Claims 22, and 35 are rejected because it is similar subject matter as claim 11.

3. Claims 6, 18, 27, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, Boneh et al. [US 7113594 B2], hereinafter Boneh, and further in view of Eisentrager et al., hereinafter Eisentrager [NPL, Eisentrager November 2003].

Regarding claim 6, Futa and Boneh teaches a method as recited by claim 5, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, and Tate pairing [US 7113594 B2, Col 2, Ln 30-40].

Futa and Boneh does not teach square pairing.

Eisentrager teaches an improved Weil and Tate pairings for elliptic and hyperelliptic curves also known as the squared Weil or squared Tate pairings [Eisentrager 2003, Pg 3, 8].

It would have been obvious to one of ordinary skilled in the art at the time of invention to combine Eisentrager pairing techniques. The suggestion/motivation would have been to have an improved pairing of the predecessors as part of the selection of the various bilinear pairing techniques. Eisentrager is an analogous art because it is in the same filed of encryption whose method can be derived from an elliptic curve when using Weil or Tate pairing.

Claims 18, 27, and 33 are rejected because it is similar subject matter as claim 6.

4. Claims 12, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Futa et al. [US 2003/0081771 A1], hereinafter Futa, and further in view of Katsura [NPL, Katsura 1975].

Regarding claim 12, Futa, and Boneh teach a method as recited by claim 1, further comprising using a trace map to shorten points on an elliptic curve mapped by the isogeny [US 7113594 B2, Col 22, Ln 27-49].

Futa and Boneh does not explicity teach an elliptic curve that is an isogeny of an Albelian variety.

Katsura teaches generating an elliptic curve mapped by isogenies of an Albelian variety [Katsura 1975, Pg 224].

It would have been obvious to one of ordinary skilled in the art at the time of invention to accommodate isogenies of an elliptic curve as taught by Katsura. The suggestion/motivation would have been to have a trace map for isogenies generated by the various techniques that comprise complex multiplication, linearly independent equations, and combinations thereof as taught by Katsura. Katsura is an analogous art because it is in the same field of generating isogenous elliptic curves.

Claim 37 is rejected because it is similar subject matter as claim 12.

5. Claims 6, 18, 27, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anonymous [NPL Anonymous, November 2003], and further in view of Eisentrager et al., hereinafter Eisentrager [NPL, Eisentrager November 2003].

Regarding claim 6, Anonymous teaches a method as recited by claim 5, wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, and Tate pairing [Anonymous, November 2003, Pg 4].

Anonymous does not explicitly teach square pairing.

Eisentrager teaches an improved Weil and Tate pairings for elliptic and hyperelliptic curves also known as the squared Weil or squared Tate pairings [Eisentrager 2003, Pg 3, 8].

It would have been obvious to one of ordinary skilled in the art at the time of invention to combine Eisentrager pairing techniques. The suggestion/motivation would have been to have an improved pairing of the predecessors as part of the selection of the various bilinear pairing techniques. Eisentrager is an analogous art because it is in the same filed of encryption whose method can be derived from an elliptic curve when using Weil or Tate pairing.

Claims 18, 27, and 33 are rejected because it is similar subject matter as claim 6.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner. Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132